*Publication des Annales des mines avec le concours du Conseil général de l'économie, de l'industrie, de l'énergie et des technologies et de l'École nationale des mines de Paris*

**N°82 • BIMESTRIEL**
**MAI 2015**

# La Gazette
## DE LA SOCIÉTÉ ET DES TECHNIQUES

**« Se défier du ton d'assurance qu'il est si facile de prendre et si dangereux d'écouter »**

*Charles Coquebert*
*Journal des mines n°1*
*Vendémiaire An III (1794)*

# Le bitcoin, de l'engouement à l'indifférence : L'avenir d'une monnaie qui a dérangé

**Créé en 2008, le bitcoin a connu un impressionnant essor médiatique fin 2013, sous l'effet d'une explosion de son cours aussi rapide qu'inattendue. L'intérêt médiatique a cependant reflué depuis juin 2014, à tel point que la perte de 5 millions de dollars en janvier 2015 par une plateforme pourtant réputée n'a guère rencontré d'écho. En février 2015, la Banque centrale européenne a publié une étude[1] à la conclusion surprenante : *« L'usage des monnaies numériques reste limité pour l'instant, impliquant une absence de danger immédiat pour les banques centrales. […] Il n'est pas à exclure qu'une nouvelle monnaie numérique, ou une amélioration substantielle puisse être une réussite dans le futur »*. Faut-il en conclure que le bitcoin a été une tentative avortée ? Une autre monnaie numérique prendra-t-elle sa place ? Le calme médiatique relatif dont il fait l'objet pourrait lui offrir l'opportunité de se défaire de sa réputation sulfureuse : 2015 marquera-t-il sa normalisation progressive ? Nombre de partisans du bitcoin lui promettent en tout cas un avenir radieux… Parce que l'aventure bitcoin met en évidence un besoin essentiel : pouvoir s'appuyer sur des monnaies à l'abri des crises systémiques des monnaies "normales".**


Au cours de l'année 2014, nous avons réalisé un mémoire de troisième année du Corps des mines sur le bitcoin ; pour cela, nous avons interrogé de nombreux acteurs et étudié maints articles et rapports d'études qui défendaient ou critiquaient cette monnaie numérique[2]. Nous avons également constaté pendant cette période combien les tempêtes médiatiques pouvaient vite se lever avant de laisser place en peu de temps au calme plat et à l'indifférence. Le calme médiatique étant revenu concernant le bitcoin, ce peut être l'opportunité de réfléchir à sa portée et à son avenir.

## Rappel : Qu'est-ce que le bitcoin[3] ?

Le bitcoin est une monnaie numérique (c'est-à-dire alternative aux principales devises officielles, et existant principalement dans le cyberespace), qui permet de réaliser *via* Internet des transactions quasi immédiates et irréversibles. Après que son principe a été décrit pour la première fois en 2008 dans un court article théorique, dans le tumulte de la crise financière, cette nouvelle monnaie fut rapidement implémentée. Les motivations de son créateur, dont l'anonymat est encore complet, restent un mystère.

### *Un fonctionnement décentralisé*

La spécificité de Bitcoin réside dans l'absence d'un tiers de confiance : c'est un algorithme décentralisé et *open source* sur un réseau informatique pair-à-pair qui permet la validation des transactions. Ce ne sont donc plus des institutions comme les banques, mais certains utilisateurs, appelés « mineurs », qui traitent les flux de transactions en temps réel.

Lors d'un transfert de bitcoins entre comptes, le détenteur du compte payeur diffuse la transaction à l'ensemble du réseau Bitcoin. Toutes les dix minutes environ, les « mineurs » regroupent les dernières transactions en un « bloc », puis les valident. Cette opération demande aux « mineurs » de mettre à disposition du réseau la puissance de calcul de leur matériel informatique. En contrepartie, le système Bitcoin les rémunère par de la création monétaire : à chaque nouvelle validation d'un bloc, de nouveaux bitcoins sont créés *ex nihilo* et distribués aux «mineurs».

Le rythme de la création monétaire est prédéterminé et décroit avec le temps, de telle sorte que la masse monétaire totale converge asymptotiquement vers le nombre manifestement arbitraire de 21 millions de bitcoins. Cette gestion très rigide de la politique monétaire, qui exclut *a priori* toute utilisation des leviers monétaires à des fins « politiques », satisfait en partie aux aspirations monétaristes d'un Milton Friedman…

## Bitcoin, comment ça marche ?

Le fonctionnement décentralisé du bitcoin (et de Bitcoin) repose sur le partage par tous les utilisateurs d'un grand livre de comptes : la *blockchain*. Celle-ci retranscrit l'intégralité des transactions ayant eu lieu depuis la création de la monnaie. Lors d'une nouvelle transaction,

elle permet de retracer l'historique du compte de l'acheteur et de vérifier qu'il dispose de fonds suffisants. Le cas échéant, la nouvelle transaction peut être validée et ajoutée à la *blockchain*.

La sécurité des transactions et la légitimité des donneurs d'ordres sont garanties par des procédés cryptographiques usuels, reposant sur des couples de clés publique et privée. Alors que l'ensemble des transactions opérées est public, chaque utilisateur possède les clés de son « compte » et est bien sûr le seul à pouvoir l'utiliser. Les bitcoins, enregistrés dans la *blockchain*, ne sont donc détenus qu'à travers la possession des clés des comptes associés.

L'un des problèmes essentiels des monnaies numériques est de prévenir la validation de transactions frauduleuses, et en particulier de la double-dépense : comment empêcher qu'un utilisateur puisse « copier » un bitcoin pour le dépenser plusieurs fois ? Bitcoin apporte une solution innovante : pour pouvoir ajouter un bloc de transactions à la *blockchain*, un « mineur » doit non seulement vérifier la validité de ces transactions, mais aussi trouver la solution à un problème arbitrairement complexe à résoudre mais dont la solution est facile à vérifier. Le premier « mineur » à achever le calcul peut alors inscrire ce nouveau bloc dans la *blockchain*, et recevoir une rémunération, dès lors que les autres « mineurs » ont reconnu l'exactitude de son calcul. Pour tromper le système, un « mineur » malveillant devrait à lui seul trouver en moyenne les solutions à tous les problèmes successifs plus rapidement que l'ensemble des « mineurs » bienveillants réunis. En pratique, le coût serait prohibitif puisque cela nécessiterait de rassembler une puissance de calcul supérieure au reste des utilisateurs. Bitcoin est donc d'autant plus sûr que le nombre de « mineurs » est important.

## Des risques pour les utilisateurs

Malgré sa forte médiatisation, le bitcoin n'a guère convaincu le grand public. Les barrières à l'entrée que constituent sa grande complexité technique ainsi que son utilité encore faible y contribuent grandement. Les risques qu'il fait peser sur les utilisateurs sont également bien réels, comme le soulignait la Banque de France dès décembre 2013[4].

***Risques financiers***

Aucune institution n'apporte sa garantie au bitcoin, aussi bien pour les « dépôts » des utilisateurs que pour la stabilité de son cours. Celui-ci a connu d'importantes variations au cours de sa jeune existence, dépassant les 1 000 $ en décembre 2013 avant de redescendre à environ 250 $ en mars 2015. Sa forte volatilité expose donc les utilisateurs au risque de pertes importantes.

Par ailleurs, en l'absence d'un animateur de marché, alors que le nombre d'utilisateurs semble encore réduit, le risque de liquidité est fortement présent. Le marché pourrait en effet s'assécher rapidement en cas d'une brusque perte de confiance, empêchant les utilisateurs de se séparer de leurs bitcoins.

***Risques techniques***

Le bitcoin est exposé à de nombreux risques opérationnels : comme tout système informatique, sa courte existence a déjà été émaillée de bugs, failles et vulnérabilités. Les utilisateurs, qu'il s'agisse d'individus ou d'entreprises spécialisées, ne sont guère épargnés par les attaques de pirates informatiques. La plupart des entreprises ne sont tenues à aucune obligation de sécurité comme peuvent l'être les banques. La faillite de la principale plateforme d'échange MtGox début 2014 et les quelques vols de bitcoin observés ensuite sur diverses plateformes (le dernier en janvier 2015) attestent de la réalité de ces risques.

Parmi les vulnérabilités du bitcoin, l'attaque dite « des 51% » est une faille majeure célèbre. Un *pool* pourrait manipuler le réseau Bitcoin à son avantage dès lors qu'il détiendrait plus de 50% de la puissance de calcul. Initialement balayée d'un revers de main, cette hypothèse a pourtant failli se concrétiser en 2014, lorsque certains *pools* se sont approchés de la barre fatidique des 51%. Jusqu'à présent, les « mineurs » se sont réorganisés pour rééquilibrer les *pools*, mais le risque n'en demeure pas moins présent.

## Faut-il avoir peur du bitcoin ?

***Anonymat et opacité des transactions***

L'anonymat constitue l'un des paradoxes du bitcoin : alors que les transactions sont publiques, les détenteurs des adresses demeurent généralement anonymes (pseudonymes en toute rigueur). Il est donc quasiment impossible de connaître la réalité économique sous-jacente à une transaction en bitcoin, à moins que l'un des utilisateurs ne se soit publiquement identifié (commerçant, bénéficiaire d'une campagne de dons…).

Les médias ont fait leurs choux gras des usages illicites supposés du bitcoin pour l'achat de drogues et d'armes, pour le blanchiment d'argent... S'il est vrai que certains sites de vente en ligne de ces produits (comme *Silkroad*) n'acceptent que des paiements en bitcoins, il convient de ne pas en tirer de conclusions trop hâtives. D'une part, l'anonymat offert par le bitcoin est tout relatif, comme le montrent les diverses arrestations de *dealers* opérant sur *Silkroad*, et d'autre part, le volume total de transactions en bitcoins est très inférieur aux estimations des transactions illégales comme le blanchiment (en 2013, entre 800 et 2 000 Mds $/an[5] contre 14 Mds $ de transactions en bitcoins). Comme le confirme la cyber-gendarmerie, le moyen le plus simple et le plus opaque pour le trafic illégal demeure l'utilisation des espèces.

***Une menace sur l'économie ?***

On se souvient des cris d'orfraie poussés par certains économistes depuis 2013 : le développement du bitcoin ferait peser un risque sur nos économies - perturbation des prix, instabilité financière… Le bitcoin mettrait en péril tous les fondements de nos systèmes économiques, en se développant en dehors de toute régulation. Le constat est désormais sans appel, confirmé par la BCE : le bitcoin et les autres monnaies virtuelles ne font peser, pour l'instant, aucun risque significatif sur nos économies.

Les raisons sont relativement simples : la masse monétaire représentée par les monnaies virtuelles est faible par rapport à celle de l'euro, leur acceptation et leur utilisation au sein du grand public restent limitées, et ces monnaies sont trop déconnectées de l'économie réelle.

> ***« Le plus simple et le plus opaque pour le trafic illégal demeure l'utilisation des espèces »***

## Comprendre l'émergence du bitcoin

***Une réussite objective***

Le succès qu'a rencontré le bitcoin depuis 2013 est indiscutable : la masse monétaire de plusieurs milliards de dollars qu'il représente, le volume journalier des transactions, l'intérêt médiatique et les investissements qu'il suscite en sont autant de preuves.

Derrière cette réussite sans précédent se cache une communication soignée : les belles promesses du bitcoin ont de quoi séduire. En tant que réseau de paiement novateur, libre et ouvert, il serait le moyen le plus simple de transférer de l'argent à peu de frais. Il n'en a pas fallu davantage pour susciter un engouement généralisé, y compris de la part des médias, fascinés par l'ingéniosité de l'algorithme et du système sur lequel repose le bitcoin.

***L'expression d'une demande pour une monnaie alternative dérégulée***

Cependant, le bitcoin est loin de tenir toutes ses promesses, et son succès actuel ne peut reposer uniquement sur l'efficacité de sa campagne marketing. Que signifie l'enthousiasme qu'il a suscité ?

Au-delà des usages opportunistes (trafic de drogue, blanchiment et spéculation), l'émergence du bitcoin traduit des tendances de fond : une perte de confiance envers les institutions, et la diffusion des idées libertariennes.

La crise financière de 2008 a écorné l'image du système bancaire international, et notamment celle des banques centrales, jugées incapables de mener une politique monétaire indépendante. Le bitcoin, reposant sur un algorithme parfaitement déterministe et décentralisé, offrait une alternative indépendante des banques centrales, insensible aux pressions politiques et au contrôle des États. Il répondait ainsi de façon concrète aux attentes de certains utilisateurs qui se méfiaient du système monétaire et bancaire traditionnel.

Le bitcoin s'est retrouvé au cœur de motivations diverses et parfois contradictoires, expliquant l'engouement médiatique et certains avis irréconciliables : suivant que l'on place davantage sa confiance dans la BCE ou dans l'algorithme Bitcoin, on ne voit pas du même œil l'absence de garantie de la banque centrale sur les dépôts en bitcoin…

Cette demande forte pour une monnaie alternative dérégulée ne doit pas être négligée si l'on souhaite bien comprendre le sens du bitcoin dans notre société et appréhender son avenir.

## Quel avenir pour le bitcoin : beaucoup de nuages…

L'indifférence médiatique dans laquelle est retombé le bitcoin et les conclusions portées par la BCE n'amènent pas à prévoir une poursuite du développement de la crypto-monnaie. Le bitcoin présente en effet certaines limites dont il lui sera difficile de s'affranchir.

### *De nombreuses limitations techniques*

Le principal frein au développement du bitcoin réside dans les contraintes techniques qui sont au cœur même de l'algorithme actuel : le nombre de transactions par seconde est limité, largement en dessous des possibilités offertes par d'autres systèmes de paiement (Visa, Mastercard), l'accroissement de la taille de la *blockchain* étant problématique…

### *La difficile équation économique du réseau Bitcoin*

Il est compliqué d'estimer le vrai coût de ce réseau basé sur une architecture décentralisée, lancé dans une course à la puissance de calcul, sans oublier le coût énergétique engendré par le matériel informatique…

En réalité, la rémunération des « mineurs » concentre les enjeux du *business model* de Bitcoin. Outre la création monétaire, qui représente actuellement l'essentiel de leur rétribution, les « mineurs » sont aussi rémunérés par l'intermédiaire des frais de transaction (faibles pour le moment). Or la création monétaire est brutalement ralentie tous les quatre ans, réduisant de moitié leur rémunération en bitcoins. Néanmoins, les « mineurs » sont tenus d'investir continuellement dans du matériel plus performant, afin de maintenir le niveau de sécurité du réseau. L'équilibre économique qui en résultera, probablement au détriment des utilisateurs qui devront payer des frais de transaction plus importants, pourrait remettre en question la pérennité de la monnaie.

### *Un problème de gouvernance*

Face aux enjeux techniques et économiques qui se présentent, la gouvernance du système Bitcoin et sa faculté à évoluer seront décisives pour son développement. Jusqu'à présent, le protocole *open source* est géré par la *Bitcoin Foundation*, porte-parole autoproclamé de la communauté Bitcoin. Si elle a dans un premier temps joué un rôle prépondérant pour le développement informatique et les actions de promotion, sa réputation a été entachée depuis fin 2013 par une série de scandales, parmi lesquels la condamnation d'un membre du *board* pour blanchiment d'argent, et par de récentes rumeurs sur une situation financière proche de la faillite. Alors que les enjeux techniques et économiques appellent une réaction ordonnée et rapide, l'absence d'une gouvernance robuste constituera vraisemblablement un obstacle majeur.

### *La question de la confiance*

Si le bitcoin offre aux yeux de certains une alternative crédible aux monnaies émises par les banques centrales, les motivations sous-jacentes au développement de cette monnaie virtuelle (libération de certaines contraintes, indépendance vis-à-vis des banques centrales) n'ont pas un fort écho auprès du grand public. Bien que le citoyen moderne soit habitué à l'utilisation de nombreuses technologies dont il ignore le fonctionnement, la monnaie jouit d'un statut à part qui se prête difficilement à la rupture de cadre conceptuel que propose le bitcoin. Peu sont enclins à transférer la confiance qu'ils ont dans les banques, toute relative soit-elle, vers un système opaque dont le fonctionnement n'est garanti par aucun État ou gouvernement. De plus, à cause de son architecture décentralisée, aucune entité ne pourrait être reconnue responsable juridiquement des dommages que pourrait causer le bitcoin.

Le souvenir de la réticence qu'a rencontrée à ses débuts la carte bancaire amène à ne pas affirmer de manière trop péremptoire que le bitcoin n'est pas prêt à convaincre le grand public ; néanmoins, il lui faudra pour cela un réel souci de pédagogie et de conviction. Il y a également fort à parier que sans un engagement des autorités, la question de la confiance pourra constituer une marche infranchissable.

## … et quelques éclaircies

***Un moyen de paiement alternatif***

Le bitcoin constitue avant tout un moyen de paiement à faible coût (pour l'instant). Son usage progresse : outre un nombre croissant de sites Internet (Overstock, Expedia, …), certains restaurants parisiens l'acceptent déjà. Ses avantages sur les offres traditionnelles des banques sont néanmoins assez limités, surtout sur Internet. Ils sont principalement liés aux transferts de fonds transfrontaliers et aux échanges au sein de communautés virtuelles. Sur le premier point, ce sont avant tout les services comme Western Union qui sont concurrencés. Par ailleurs, le bitcoin pourrait constituer une alternative intéressante dans des pays au système bancaire peu développé.

***De nouvelles fonctionnalités***

Bitcoin est également le porteur potentiel d'innovations financières : le *crowdfunding* (cf. gazette de septembre 2014) en est ainsi une fonctionnalité native. Les transactions en bitcoins peuvent être assorties de conditions et rendre ainsi des services plus évolués que les moyens de paiement traditionnels, sans même recourir à des tiers de confiance (caution, transaction sous séquestre). Cependant, si ces fonctionnalités sont déjà présentes dans le protocole, leur utilisation est pour l'instant peu intuitive et reste inaccessible au grand public.

Il existe par ailleurs de nombreuses autres possibilités offertes par le protocole, plus éloignées des usages monétaires et financiers, et basées sur le principe de décentralisation. En particulier, Bitcoin pourrait évoluer pour jouer le rôle d'une plateforme hébergeant une multitude de services qui restent encore à imaginer : courriels, réseau social... La *blockchain* ouvre de nombreuses opportunités aux entrepreneurs inventifs.

***D'innombrables émules***

Signe de l'intérêt porté au bitcoin, le secteur des monnaies numériques a explosé depuis 2013 : en février 2015, on en dénombre plus de 500 basées sur le modèle du bitcoin. Seul un petit nombre d'entre elles apporte quelques nouveautés : certaines corrigent des « défauts », d'autres proposent de nouvelles fonctionnalités, d'autres encore reposent sur de nouveaux systèmes de validation. Néanmoins, le bitcoin bénéficie toujours d'une longueur d'avance grâce au réseau qu'il a constitué.

***Un écosystème innovant et dynamique***

Tout un écosystème s'est progressivement développé afin de fournir de nouveaux services aux utilisateurs de bitcoins.

La course à la puissance de calcul a stimulé la création de nombreuses sociétés spécialisées dans le développement et la vente de matériel dédié, ainsi que dans la location de puissance de calcul à travers le *Cloud*.

L'intérêt du bitcoin dépendant directement de l'usage qui peut en être fait, des solutions sont rapidement apparues afin d'en faciliter l'adoption par les utilisateurs privés et professionnels. Face au risque de perte des clés des comptes en bitcoins, par suite d'une défaillance informatique ou d'un piratage, de nombreux systèmes de portefeuille électronique se sont développés pour permettre aux utilisateurs de stocker leurs clés en toute sécurité. En parallèle, des prestataires de services de paiement, tel BitPay, proposent des solutions d'intermédiation des transactions à destination des commerçants, leur permettant d'accepter les paiements en bitcoins de manière transparente.

Les plateformes de change constituent un outil indispensable en assurant la conversion avec les autres devises. Elles centralisent et confrontent l'offre et la demande à travers un mécanisme de marché, déterminant ainsi le cours du bitcoin. Alors qu'il se posait initialement comme une alternative aux excès de la finance et à la faiblesse des institutions financières, le bitcoin n'a pu éviter le développement de plateformes promouvant ces dérives qu'il dénonçait. De plus en plus de sites tels que iCBIT ou bitcoin-otc voient le jour depuis 2014, proposant des plateformes de *trading* en bitcoin et des produits dérivés de gré-à-gré. En janvier 2015, Coinbase a annoncé l'ouverture de la première plateforme de change, respectant la réglementation financière aux États-Unis, signe de la vitalité de la monnaie.

Toutes ces entreprises ont émergé en un temps record. Loin de tarir, les *start-ups* dédiées à Bitcoin continuent de lever des montants astronomiques auprès d'investisseurs. Ainsi, la start-up *21 Inc.*, dont le *business model* est gardé secret, a récolté récemment 105 M$.

## États et bitcoin, une position à clarifier

*Wait and see* : telle est la position proposée par la BCE dans son étude. Cette position d'attentisme semble assez risquée. Cependant, la réticence des États à clarifier le statut du bitcoin est vraisemblablement due à la volonté de ne pas reconnaître, même implicitement, les monnaies virtuelles, de peur de favoriser leur essor et de se lier les mains en définissant un statut juridique inadapté ou trop peu flexible.

Sous l'impulsion d'un mouvement structurel de demande d'une monnaie alternative dérégulée, l'émergence du bitcoin a été extrêmement rapide ; il n'est pas à exclure que des monnaies alternatives soient adoptées à une échelle beaucoup plus large dans un délai très bref. Il conviendrait donc d'établir dès à présent un cadre légal pour réguler les monnaies numériques. Ces régulations et, éventuellement, restrictions d'usage devront être imaginées au niveau international. Toute tentative locale ou même européenne serait rapidement sans effet, les acteurs pouvant s'implanter en dehors du contrôle des différentes autorités prudentielles ou de régulation. Des autorités internationales étudient de près ces possibilités, sans toutefois porter de conclusions concrètes pour l'instant.

Quelles que soient les motivations à l'origine du bitcoin et les moteurs de son essor, les États ont un rôle important à jouer dans son développement. Si certains usages opportunistes sont à limiter, d'autres innovations sont à promouvoir, innovations qui vont au-delà de la sphère monétaire.

*Nicolas Clausset et Arnaud Sellem, ingénieurs des mines*

## NOTE

[1] European Central Bank : "Virtual currency schemes – A further analysis", Février 2015

[2] Mémoire de troisième année, "Bitcoin un essai à transformer, Histoire immédiate d'une monnaie qui dérange", Ecoles des mines de Paris

[3] Il est d'usage de distinguer le bitcoin, en tant que monnaie virtuelle, de l'algorithme et du réseau sous-jacent, que l'on désigne par le terme Bitcoin (avec majuscule mais sans article). La différence entre Bitcoin et le bitcoin semble parfois ténue, compte tenu de l'intrication de la monnaie et du protocole.

[4] Banque de France : Focus n°10 – 5 décembre 2013 : "Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin"

[5] *Source : United Nations Office on drugs and crimes*


***La Gazette de la société et des techniques***

La *Gazette de la Société et des Techniques* a pour ambition de faire connaître des travaux qui peuvent éclairer l'opinion, sans prendre parti dans les débats politiques et sans être l'expression d'un point de vue officiel. Elle est diffusée par abonnements gratuits. Vous pouvez en demander des exemplaires ou suggérer des noms de personnes que vous estimez bon d'abonner.

Vous pouvez consulter tous les numéros sur le web à l'adresse :
**http://www.annales.org/gazette.html**

**RENSEIGNEMENTS ADMINISTRATIFS**
**Dépôt légal mai 2015**

***La Gazette de la Société et des techniques***
est éditée par les *Annales des mines*,
120, rue de Bercy - télédoc 797 - 75012 Paris
http://www.annales.org/gazette.html
Tél. : 01 42 79 40 84
Fax : 01 43 21 56 84 - mél : michel.berry@ensmp.fr
N° ISSN 1621-2231.
**Directeur de la publication :** Pierre Couveinhes
**Rédacteur en chef :** Michel Berry
**Illustrations :** Véronique Deiss
**Réalisation :** PAO - SG - SEP 2 C
**Impression :** France repro

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
DE L'INDUSTRIE ET DU NUMÉRIQUE